REMARKS/ARGUMENTS

The Final Office Action of September 13, 2005, has been carefully reviewed and these remarks are responsive thereto. Applicant requests entry of the amendment and following remarks to place the application in condition for allowance or better form for appeal.

Claims 1, 4, 6, 8, 10-11, 14-16, 18-19, and 23 have been amended. Claims 2-3, 5, 12-13, 20-22, and 24-26 have been cancelled. Claims 1, 4, 6-11, 14-19, 23, and 27-35 are pending in this application. Reconsideration and allowance of the instant application are respectfully requested.

Rejection of Claim 22 Under 35 U.S.C. § 112, Second Paragraph

Claim 22 stands rejected under 35 U.S.C. § 112, second paragraph. Applicants have amended claim 22 to overcome this rejection.

Rejection of Claims Under 35 U.S.C. § 102 (e) over Geiger et al.

Claims 1, 4, 6-11, 14-19, 23, and 27-35 stand rejected under 35 U.S.C. § 102 (e) over Geiger et al. Applicant traverses the rejection.

Claim 1 recites:

> " receiving at said token an authentication of said control point and an authentication of said token;
>
> transmitting to said control point said authentication of said token, …"

Geiger et al. discloses all transmissions between the wireless device 450 and all other components to be in a common network. Importantly, the Attribute Authorities 404-406 obtain their authentication of the token by one of two ways. First, the Attribute Authorities 404-406 directly compute the authentication of the wireless device from the PKI certificate received from the wireless device. See step 545 of Figure 5 and column 13, lines 57-60. Second, the Attribute Authorities 404-406, when using separate validation servers as described in column 15, line 62, through column 17, line 13, provide the certificates to other trusted entities to perform the

validation. Importantly, the Attribute Authorities 404-406 use their own trusted pathways for the authentication of the wireless device. In other words, the control points use their own trusted pathways to authenticate the token.

Claim 1 has been amended to more clearly recite the invention as set forth above. Geiger fails to disclose "receiving at said token an authentication of … said token" and "transmitting to said control point said authentication of said token" as currently recited in claim 1. Accordingly, claim 1 is allowable over Geiger et al.

Claims 4 and 6-9 are allowable for at least the reasons set forth above.

Claim 10 recites:

> " transmitting said obtained information regarding said control point and information regarding said token to said network via said control point;
>
> via said control point, receiving at said token authentication information of said control point, said authentication information relating to said database of approved control points and having been received from said network connectable to said control point, …"

Geiger et al. discloses two ways of authenticating the Attribute Authorities 404-406. First, the wireless device can authenticate the Attribute Authorities 404-406 in the wireless device itself based on a received certificate from the Attribute Authority. See steps 515 and 520 of Figure 5 and column 13, lines 26-29. Second, the wireless device can use a separate validation server when acting in a thin client mode. See column 15, line 62, through column 17, line 13. In short, the wireless device always uses its own trusted infrastructure to validate the Attribute Authority.

Claim 10 has been amended to recite that "via said control point, receiving at said token authentication information of said control point". Geiger et al. fails to disclose claim 10 as now amended. Accordingly, claim 10 is allowable over Geiger et al.

Claims 11 and 14-19 are similarly allowable over Geiger et al.

Claim 23 recites:

> "said wireless communication portion configured to transmit authentication of said device to the control point after having been received from said network …"

Similar to the difference between Geiger et al. and claim 1 raised above, Geiger et al. fails to disclose the Attribute Authorities 404-406 receiving "authentication of said device …after having been received from said network". Accordingly, claim 23 is allowable over Geiger et al.

Claims 27-32 are allowable for at least the reasons described above.

Claim 33 recites:

> " obtaining access to said physical location beyond said control point."

Geiger et al. only discloses on-line, remotely located Attribute Authorities 404-406 that provide downloadable content. Claim 33 relates to access control to a physical location. Geiger et al. is devoid of access control to a physical location as now claimed.

Claims 34-35 are allowable for at least the reasons set forth above.

All rejections having been addressed, applicant respectfully submits that the instant application is in condition for allowance, and respectfully solicits prompt notification of the same. However, if for any reason the Examiner believes the application is not in condition for allowance or there are any questions, the Examiner is requested to contact the undersigned at (202) 824-3184.

Respectfully submitted,
BANNER & WITCOFF, LTD.

Dated: February 13, 2006

By: /Christopher R. Glembocki/
Christopher R. Glembocki
Registration No. 38,800

1001 G Street, N.W.
Washington, D.C. 20001-4597
(202) 824-3000